

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2000-332745
(P2000-332745A)

(43)公開日 平成12年11月30日 (2000.11.30)

(51)Int.Cl. ⁷	識別記号	F I	マーク* (参考)
H 04 L 9/14		H 04 L 9/00	6 4 1 5 C 0 6 4
H 04 H 1/00		H 04 H 1/00	F 5 J 1 0 4
H 04 J 3/00		H 04 J 3/00	M 5 K 0 2 8
H 04 L 12/56		H 04 L 11/20	B 5 K 0 3 0
			1 0 2 Z
	審査請求 未請求 請求項の数10 O L (全 12 頁)		最終頁に続く

(21)出願番号 特願平11-140340

(22)出願日 平成11年5月20日 (1999.5.20)

(71)出願人 000006013

三菱電機株式会社

東京都千代田区丸の内二丁目2番3号

(72)発明者 松崎 一博

東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(72)発明者 加藤 嘉明

東京都千代田区丸の内二丁目2番3号 三菱電機株式会社内

(74)代理人 100066474

弁理士 田澤 博昭 (外1名)

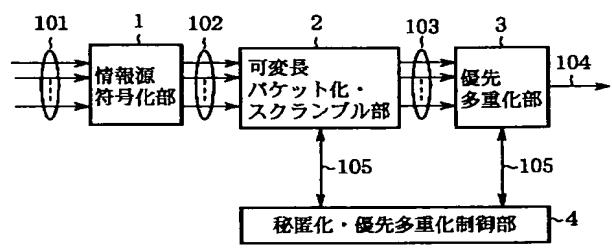
最終頁に続く

(54)【発明の名称】 限定受信方式の送信装置および受信装置

(57)【要約】

【課題】 多重化遅延時間に比較してスクランブル鍵の更新周期が比較的小さい場合には、古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが混在して、受信側で復号不能になるという課題があった。

【解決手段】 情報源符号化部1と、可変長パケット化・スクランブル部2と、優先多重化部3と、秘匿化・優先多重化制御部4とを有する限定受信方式の送信装置において、秘匿化・優先多重化制御部4が、多重化ビット列104において最大多重化遅延時間よりも大きな時間間隔でスクランブル鍵を更新するように制御する。



- 1: 情報源符号化部 (情報源符号化手段)
- 2: 可変長パケット化・スクランブル部 (パケット化・スクランブル手段)
- 3: 優先多重化部 (優先多重化手段)
- 4: 秘匿化・優先多重化制御部 (秘匿化・優先多重化制御手段)

101: コンテンツ
102: 情報源符号化ビット列
103: 可変長パケット列 (パケット列)
104: 多重化ビット列
105: ~

【特許請求の範囲】

【請求項1】 各種のコンテンツを符号化する情報源符号化手段と、

該情報源符号化手段から出力される情報源符号化ビット列をパケットに格納するとともに該パケットの一部分を秘匿化してパケット列を生成するパケット化・スクランブル手段と、

複数の情報源符号化ビット列を該情報源符号化ビット列毎に与えられた多重化遅延に基づく優先度に基づいてパケット単位に多重化して多重化ビット列を生成する優先多重化手段と、

前記パケット化・スクランブル手段および前記優先多重化手段を制御する秘匿化・優先多重化制御手段とを有する限定受信方式の送信装置において、

前記秘匿化・優先多重化制御手段が、前記多重化ビット列において、最大多重化遅延時間よりも大きな時間間隔でスクランブル鍵を更新するように制御することを特徴とする限定受信方式の送信装置。

【請求項2】 パケット化・スクランブル手段が、情報源符号化ビット列を可変長パケットのペイロードに格納して可変長パケットを生成することを特徴とする請求項1記載の限定受信方式の送信装置。

【請求項3】 各種のコンテンツを符号化する情報源符号化手段と、該情報源符号化手段から出力される情報源符号化ビット列をパケットに格納するとともに該パケットの一部分を秘匿化してパケット列を生成するパケット化・スクランブル手段と、

複数の情報源符号化ビット列を該情報源符号化ビット列毎に与えられた多重化遅延に基づく優先度に基づいてパケット単位に多重化して多重化ビット列を生成する優先多重化手段と、

前記パケット化・スクランブル手段および前記優先多重化手段を制御する秘匿化・優先多重化制御手段とを有する限定受信方式の送信装置において、

前記パケット化・スクランブル手段が、パケットの一部を秘匿化するために使用したスクランブル鍵を格納するECMを特定するためのECM特定番号をパケットのヘッダに登録することを特徴とする限定受信方式の送信装置。

【請求項4】 パケット化・スクランブル手段が、情報源符号化ビット列を可変長パケットのペイロードに格納して可変長パケットを生成することを特徴とする請求項3記載の限定受信方式の送信装置。

【請求項5】 パケット単位に多重化遅延に基づく優先度に応じて多重化された多重化ビット列をコンテンツ毎のパケット列に分離する優先多重分離手段と、

パケット列において秘匿化された部分の秘匿を解除するとともに、パケットを分解して情報源符号化ビット列を生成するパケット分解・デスクランブル手段と、

情報源符号化ビット列を復号してコンテンツを再生する情報源復号手段とを有する限定受信方式の受信装置において、

前記パケット分解・デスクランブル手段が、ECM特定番号を参照して、パケットの一部分を秘匿化するために使用したスクランブル鍵を特定し、パケットの秘匿化部分の秘匿を解除することを特徴とする限定受信方式の受信装置。

【請求項6】 各種のコンテンツを符号化する情報源符号化手段と、

該情報源符号化手段から出力される情報源符号化ビット列をパケットに格納して該パケットの一部分を秘匿化するパケット化・スクランブル手段と、

複数の情報源符号化ビット列を該情報源符号化ビット列毎に与えられた多重化遅延に基づく優先度に基づいてパケット単位に多重化して多重化ビット列を生成する優先多重化手段と、

前記パケット化・スクランブル手段および前記優先多重化手段を制御する秘匿化・優先多重化制御手段とを有する限定受信方式の送信装置において、

前記秘匿化・優先多重化制御手段が、秘匿化についての優先度に基づいてパケットの秘匿特性を制御することを特徴とする限定受信方式の送信装置。

【請求項7】 秘匿化・優先多重化制御手段は、コンテンツ毎の情報源符号化モード単位に設定された秘匿化についての優先度に基づいてパケットの秘匿特性を制御することを特徴とする請求項6記載の限定受信方式の送信装置。

【請求項8】 秘匿化・優先多重化制御手段は、秘匿化についての優先度に基づき、暗号の種類、およびCBCモードやOFBモード等の暗号の利用モードを変えて暗号化することを特徴とする請求項6または請求項7に記載の限定受信方式の送信装置。

【請求項9】 秘匿化・優先多重化制御手段は、秘匿化についての優先度に基づき、秘匿化期間を制御することを特徴とする請求項6または請求項7に記載の限定受信方式の送信装置。

【請求項10】 パケット化・スクランブル手段が、情報源符号化ビット列を可変長パケットのペイロードに格納して可変長パケットを生成することを特徴とする請求項6から請求項9のいずれか1項に記載の限定受信方式の送信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、デジタル化された映像信号、音響信号、その他データ等のマルチメディアデータを符号化および多重化して伝送する際に、信号をスクランブルして秘匿化し、予め契約を結んだ特定の受信者のみがスクランブル信号を復号できる限定受信方式の送信装置および受信装置に関するものである。

【0002】

【従来の技術】図10は、例えば片方善治監修「マルチメディア産業応用技術体系」pp. 495~496、フジ・テクノシステム(1997年)に示された従来の限定受信方式の送信装置の構成を示すブロック図である。また、図11は、同様に上記文献に示された従来の限定受信方式の受信装置の構成を示すブロック図である。

【0003】図10において、21は情報源符号化部、22は固定長パケット化・スクランブル部、23は多重化部、24は秘匿化・多重化制御部である。また、401は映像信号、音声信号、種々のデータ等のコンテンツ、402は情報源符号化ビット列、403は固定長パケット列、404は多重化ビット列、405は秘匿化・多重化のための制御信号である。なお、図において矢印はそれぞれのコンテンツまたは符号化処理されたビットストリームの伝送路を示し、情報源符号化部21等では、複数の伝送路により伝送される複数のコンテンツまたはビットストリームが並列に処理される。図11において、25は多重分離部、26は固定長パケット分解・デスクランブル部、27は情報源復号部である。

【0004】次に動作について説明する。まず、従来の限定受信方式の送信装置における処理について図10を参照して説明する。情報源符号化部21は、映像信号、音声信号、データ等の複数のコンテンツ401に対して情報源符号化処理を行なって情報源符号化ビット列402を生成する。固定長パケット化・スクランブル部22は、それぞれの情報源符号化ビット列402を適切に分割して固定長パケットのペイロードに格納して固定長パケットを生成するとともに、固定長パケットのペイロードをスクランブル処理して秘匿化し固定長パケット403を生成する。さらに、固定長パケット化・スクランブル部22は、コンテンツに対する情報源符号化ビット列402をペイロードに格納した通常の固定長パケットに加えて、スクランブル鍵などの秘匿化情報をECM(Entitlement Control Message)として固定長パケットに格納して出力する。多重化部23は、固定長パケット列403を固定長パケット単位に多重化して多重化ビット列404を生成する。また、秘匿化・多重化制御部24は、秘匿に使用するスクランブル鍵の更新タイミング、ECMの多重化タイミング等を制御する。

【0005】次に、従来の限定受信方式の受信装置における処理について図11を参照して説明する。従来の限定受信方式の受信装置における処理は、送信装置における処理と逆の処理となる。図11に示されるように、多重分離部25は多重化ビット列404をコンテンツ毎に分離して、それぞれのコンテンツに対応した複数の固定長パケット列403を生成する。固定長パケット分解・デスクランブル部26は、ECMとして送られてきた秘*

$T_s - 2T_t - \Delta T \leq T_{ecm} < T_s - \Delta T$ (式1)
を少なくとも満足する必要がある。ここで、 $2T_t$ は、

* 匿化情報を用いて固定長パケット列403の秘匿状態を解除するとともに、パケットを分解して情報源符号化ビット列402を生成する。情報源復号部27は、情報源符号化ビット列402を復号して、映像信号、音声信号、種々のデータ等のコンテンツ401を再生する。

【0006】さらに、従来の限定受信方式における伝送信号の多重方式、及び秘匿化・多重化制御部24の動作について説明する。図12は、例えば電波産業界標準規格「BSデジタル放送の送信・運用条件(A R I B S 10 TD-B20 1.0版)」pp. 20~38(1998年11月6日)に示された従来の限定受信方式における伝送信号の多重方式を説明する図である。なお、多重化に関して、送信装置における処理と受信装置における処理とは逆の処理となるので、ここでは送信装置における処理について説明する。

【0007】コンテンツ毎(情報源毎)のそれぞれの情報源符号化ビット列402を固定長のパケットに分割し、パケットのペイロードに対してスクランブル処理を施し、スクランブルされた固定長パケットをパケット単位に多重化して多重化ビット列404を生成する。スクランブル鍵等の秘匿化情報は、ECMとして固定長パケットに格納して多重化する。ECMは、コンテンツ毎に指定することも、複数コンテンツに共通なものとして指定することも可能である。また、ECMは周期的(時間間隔: t)に送出される。1つのECMにより、それぞれ奇数鍵(odd key)および偶数鍵(even key)と呼ばれて区別される2種類のスクランブル鍵が同時に運ばれる。ECMに格納された奇数鍵と偶数鍵とは同時に更新されずに、1つずつ順番に更新される。

【0008】秘匿化するか否かについての秘匿化/非秘匿化情報、秘匿化に使用したスクランブル鍵の種別(奇数鍵/偶数鍵)情報は、固定長パケット単位に付加することが可能である。これら秘匿化に関する情報は、固定長パケットのヘッダに格納される。

【0009】秘匿化に関する設定内容が更新されたECMを格納するパケットの直後に、更新した鍵を使用してスクランブル処理を実施したパケットを多重化して伝送した場合には、受信側では更新された鍵の取り込みが間に合わずデスクランブルエラーが生じることがある。

40 そのために、内容更新のあったECMを格納するパケットと、更新した鍵でスクランブルされたパケットとは、通常、受信側における鍵取り込み時間を考慮して時間間隔を開けて多重化される。例えば、更新したスクランブル鍵をECMで送る時刻を T_{ecm} 、更新したスクランブル鍵の受信側での使用時刻を T_s 、スクランブル鍵の更新周期を T_t 、多重化遅延を考慮しない転送時間を含めた受信側における鍵の取り込み時間を ΔT とすると、

$$T_s - 2T_t - \Delta T \leq T_{ecm} < T_s - \Delta T$$

50 受信側において奇数鍵または偶数鍵の使用が有効な期間

として与えられるものである。すなわち、送信側では、更新周期 T_t ごとに奇数鍵から偶数鍵へまたは偶数鍵から奇数鍵へスクランブル鍵が更新されて、更新されたスクランブル鍵を基にしてスクランブル処理がなされる。しかし、奇数鍵から次の奇数鍵への更新または偶数鍵から次の偶数鍵への更新は $2T_t$ を周期として実施され、また各パケットには使用されるスクランブル鍵の種別（奇数鍵または偶数鍵）が登録されているから、受信側におけるスクランブル鍵の使用有効期間は $2T_t$ となる。そして、秘匿化・多重化制御部24は、式1を満足するように、スクランブル鍵の更新周期、ECMの更新タイミング等を制御する。

【0010】

【発明が解決しようとする課題】従来の限定受信方式の送信装置等は以上のように構成されているので、情報源符号化ビット列を分割して固定長パケットのペイロードに格納する際に、パケットを固定長にするためにダミーバイトを挿入する必要があり、多重化の効率が低下するという課題があった。

【0011】また、従来の限定受信方式の送信装置等では、多重化に関して優先度が付された情報源符号化ビット列を秘匿化して多重化伝送する場合、優先度の低いパケットの多重化遅延時間に比較してスクランブル鍵の更新周期 T_t が比較的小さい場合には、受信側では古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが混在して届くために復号不能になるという課題があった。

【0012】また、従来の限定受信方式の送信装置等では、コンテンツ毎の情報源符号化モードに応じて秘匿化の優先度を設定することはなかったので、それぞれの情報源符号化モードに応じて柔軟な秘匿特性を設定することができないという課題があった。ここで、秘匿特性とは、コンテンツを秘匿化する期間設定、秘匿化に用いられる暗号の種類、及びCBC (Cipher Block Chaining) モードやOFB (Output Feed Back) モード等の暗号の利用モード等の秘匿化に関する属性全般を指すものである。また、情報源符号化モードとは、各コンテンツを符号化する際の符号化方式を示すものであり、MPE-G-2ビデオ規格を例にとれば、イントラ予測モード、前方向予測モードおよび両方向予測モードが符号化モードとして与えられている。

【0013】この発明は上記のような課題を解決するためになされたもので、複数の情報源符号化ビット列をパケットに格納するとともに秘匿化して多重化伝送する際に、多重化の効率を向上させた限定受信方式の送信装置および受信装置を得ることを目的とする。

【0014】また、この発明は、新しい鍵でスクランブルされたパケットと古い鍵でスクランブルされたパケットとの混在等による復号不能を防止して、信頼性の高い限定受信方式の送信装置および受信装置を得ることを目

的とする。

【0015】さらに、この発明は、コンテンツ毎の情報源符号化モードに応じて柔軟な秘匿特性を設定できる限定受信方式の送信装置および受信装置を得ることを目的とする。

【0016】

【課題を解決するための手段】この発明に係る限定受信方式の送信装置は、秘匿化・優先多重化制御手段が多重化ビット列において、最大多重化遅延時間よりも大きな時間間隔でスクランブル鍵を更新するように制御するものである。

【0017】この発明に係る限定受信方式の送信装置は、パケット化・スクランブル手段が情報源符号化ビット列を可変長パケットのペイロードに格納して可変長パケットを生成するようにしたものである。

【0018】この発明に係る限定受信方式の送信装置は、パケット化・スクランブル手段がパケットの一部分を秘匿化するために使用したスクランブル鍵を格納するECMを特定するためのECM特定番号をパケットのヘッダに登録するようにしたものである。

【0019】この発明に係る限定受信方式の受信装置は、パケット分解・デスクランブル手段が、ECM特定番号を参照して、パケットの一部分を秘匿化するために使用したスクランブル鍵を特定し、パケットの秘匿化部分の秘匿を解除するようにしたものである。

【0020】この発明に係る限定受信方式の送信装置は、秘匿化・優先多重化制御手段が秘匿化についての優先度に基づいてパケットの秘匿特性を制御するようにしたものである。

【0021】この発明に係る限定受信方式の送信装置は、秘匿化・優先多重化制御手段がコンテンツ毎の情報源符号化モード単位に設定された秘匿化についての優先度に基づいてパケットの秘匿特性を制御するようにしたものである。

【0022】この発明に係る限定受信方式の送信装置は、秘匿化・優先多重化制御手段が秘匿化についての優先度に基づき、暗号の種類、およびCBCモードやOFBモード等の暗号の利用モードを変えて暗号化するようにしたものである。

【0023】この発明に係る限定受信方式の送信装置は、秘匿化・優先多重化制御手段が秘匿化についての優先度に基づき秘匿化期間を制御するようにしたものである。

【0024】

【発明の実施の形態】以下、この発明の実施の一形態を説明する。

実施の形態1、図1は、この発明の実施の形態1による限定受信方式の送信装置の構成を示すブロック図である。また、図2は、この発明の実施の形態1による限定

50 受信方式の受信装置の構成を示すブロック図である。

【0025】図1において、1は各種コンテンツ情報に対して符号化処理を行なう情報源符号化部（情報源符号化手段）、2は可変長パケット化および秘匿化を実施する可変長パケット化・スクランブル部（パケット化・スクランブル手段）、3は優先度に応じて多重化を実施する優先多重化部（優先多重化手段）、4は可変長パケット化・スクランブル部2および優先多重化部3を制御する秘匿化・優先多重化制御部（秘匿化・優先多重化制御手段）である。また、101は映像信号、音声信号、種々のデータ等のコンテンツ、102は情報源符号化ビット列、103は可変長パケット列（パケット列）、104は多重化ビット列、105は秘匿化・優先多重化のための制御信号である。

【0026】図2において、5は多重化ビット列104をコンテンツ毎に可変長パケット列103に分離する優先多重分離部（優先多重分離手段）、6は秘匿を解除するとともに可変長パケットを分解して情報源符号化ビット列102を生成する可変長パケット分解・デスクランブル部（パケット分解・デスクランブル手段）、7は情報源符号化ビット列102を復号してコンテンツ101を再生する情報源復号部（情報源復号手段）である。

【0027】次に動作について説明する。第1に、この発明の実施の形態1による限定受信方式の送信装置における処理について図1を参照して説明する。情報源符号化部1は、映像信号、音声信号、データ等の複数のコンテンツ101に対して情報源符号化処理を行なって情報源符号化ビット列102を生成する。この符号化処理を実施するに際して、映像信号の情報源符号化についてはMPEG-2ビデオ規格に準拠しており、映像フレーム、映像フィールド等に相当する「ピクチャ」と呼ばれる符号化ユニットを単位として、イントラ予測モード、前方向予測モード、両方向予測モードの中から情報源符号化モードが選択される。一方、音声信号、種々のデータ等に関しては、所定の時間長や所定のバイト長を符号化ユニットとして情報源符号化処理が実施される。

【0028】次に、可変長パケット化・スクランブル部2は、それぞれの情報源符号化ビット列102を符号化ユニット毎に分割して可変長パケットのペイロードに格納して可変長パケットを生成するとともに、可変長パケットのペイロードをスクランブル処理して秘匿化し可変長パケット列103を生成する。

【0029】図3は、この発明の実施の形態1により使用される可変長パケットの構成を示す図である。201は可変長パケットの先頭を識別するためのユニークワードが格納されたパケットスタートコード、202はパケットに格納されるコンテンツ毎に異なる番号が付与されるパケット識別子、203は秘匿化／非秘匿化情報、秘匿化に使用する奇数鍵／偶数鍵の区別情報、CBCやOFB等の暗号の利用モード等を通知する秘匿化情報、204は当該可変長パケットの秘匿化に係るECMを格納

する可変長パケットのパケット識別子の値を通知するECM識別番号、205は可変長パケットのペイロード長を示すペイロード長、206は可変長パケットのヘッダ部分の誤りチェック、およびスクランブル処理を行なった際のパケットスタートコード201とのエミュレーションを防止するために付与されたCRC、207は符号化されたビット列を格納する可変長パケットペイロードである。なお、コンテンツまたは情報源符号化モード等に応じて種別の異なる複数のECMが用意されており、10 ECM識別番号204により、当該パケットに係るコンテンツまたは情報源符号化モードに応じたECMの種別が識別される。

【0030】秘匿化の際には、秘匿化・優先多重化制御部4から出力される制御信号105により、コンテンツ内容に応じて、あるいは符号化ユニット毎の情報源符号化モードに応じて、秘匿化に使用する暗号の種類、CBCやOFB等の暗号の利用モード、秘匿化／非秘匿化情報等が可変長パケット毎に制御されて、これら制御情報がそれぞれの可変長パケットの秘匿化情報203のフィールドに書き込まれる。

【0031】例えば、映像コンテンツの場合、秘匿化・優先多重化制御部4は、秘匿化について符号化ユニットの情報源符号化モードに対して規定される以下のようない優先度Pcaに基づき、次のように制御する。

Pca=1：全ての符号化ユニットを秘匿化。

Pca=2：イントラ予測モード以外の符号化ユニットを秘匿化。

Pca=3：両方向予測モードの符号化ユニットのみ秘匿化。

Pca=4：秘匿化なし。

【0032】また、音声コンテンツや種々のデータコンテンツに対する秘匿化については、秘匿化・優先多重化制御部4は、秘匿化の優先度に応じて、秘匿化期間または非秘匿化期間を符号化ユニット単位に制御する。また、秘匿化の優先度によっては、使用する暗号の種類を変えたり、CBCモードやOFBモード等の暗号の利用モードを変えることによって秘匿の強度を制御する。なお、秘匿化に関して個々の可変長パケットの秘匿化情報203のフィールドに収容されないスクランブル鍵等の40 秘匿化関連情報は、ECMとして可変長パケットのペイロードに格納して送られる。

【0033】次に、優先多重化部3は、コンテンツ毎の可変長パケット列103を優先多重化して、固定ビットレート(CBR)の多重化ビット列104を生成する。この際、優先多重化時の多重化特性は、各コンテンツに与えられた多重化遅延に関する優先度に基づいて制御信号105により制御される。多重化遅延に関する優先度は、ECMおよび制御情報を最優先とする。また、リアルタイム伝送が必要なコンテンツに対する優先度を高くするとともに、リアルタイム伝送を必要とはしないコン

コンテンツに対する優先度を低くする。さらに、映像と当該映像に付随する音声との場合のように、同期再生が必要となる複数のコンテンツには同じ優先度を与える。

【0034】また、秘匿化・優先多重化制御部4は、既に述べた可変長パケット毎の秘匿化優先度の制御に加えて、秘匿に使用するスクランブル鍵の更新タイミングの制御、ECMの多重化タイミングの制御、各コンテンツに与えられた多重化遅延に関する優先度に基づく優先多重化制御等を行なう制御信号105を出力する。

【0035】第2に、この発明の実施の形態1による限定受信方式の受信装置における処理について図2を参照して説明する。図2に示されるように、優先多重分離部5は、パケットスタートコード201、パケット識別子202、ペイロード長205、およびCRC206を参照して、多重化ビット列104をコンテンツ毎に分離して可変長パケット列103を生成する。

【0036】次に、可変長パケット分解・デスクランブル部6は、秘匿化情報203とECM識別番号204により同定されたECMとを参照して可変長パケットのペイロードの秘匿を解除するとともに、可変長パケットを分解してコンテンツ毎の情報源符号化ビット列102を生成する。そして、情報源復号部7は、情報源符号化ビット列102を復号して映像信号、音声信号、種々のデータ等のコンテンツ101を再生する。

【0037】第3に、この発明の実施の形態1による限定受信方式における伝送信号の多重方式、及び秘匿化・優先多重化制御部4の動作について説明する。図4は、この発明の実施の形態1による限定受信方式における伝送信号の多重方式を説明する図である。なお、多重化に関して、送信側の処理と受信側の処理とは逆の処理となるので、ここでは送信側の処理に基づいて説明する。

【0038】コンテンツ毎の（情報源毎）のそれぞれの*

$$T_t > T_{dmx}$$

を満足するように、スクランブル鍵の更新周期 T_t を制御する。

【0042】既に述べたように、送信側において奇数鍵から偶数鍵へまたは偶数鍵から奇数鍵へスクランブル鍵が更新される周期は T_t であるが、受信側における奇数鍵または偶数鍵の使用有効期間は $2T_t$ であるので、例え送信側で更新直前のスクランブル鍵によりスクランブルされたパケットが多重化遅延により受信側に遅れて到着したとしても、その遅延時間が T_t 以内であれば受信側でデスクランブル処理が可能であるから、式1および式2を満たすように制御することで、古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが受信側で混在することが防止される。

【0043】 T_{dmx} に関しては、優先多重化シミュレーション等によって見積もった値を使用してもよいし、多重化遅延に関する閾値制御を行なって各パケットの多重化遅延が T_{dmx} を超えないようにしてもよい。

* 情報源符号化ビット列102を符号化ユニット毎に可変長のパケットに格納し、パケットのペイロードに対してスクランブル処理を施し、コンテンツ毎に与えられた多重化遅延に関する優先度に基づいてスクランブル処理された可変長パケットをパケット単位に多重化して多重化ビット列104を生成する。スクランブル鍵等の秘匿化情報は、ECMとして可変長パケットに格納して多重化する。

【0039】この発明の実施の形態1による限定受信方式では、ECMはコンテンツ毎に指定することも、複数コンテンツに共通なものとして指定することも可能である。また、ECMは周期的（時間間隔： t ）に送出される。1つのECMにより、それぞれ奇数鍵および偶数鍵と呼ばれて区別される2種類のスクランブル鍵が同時に運ばれる。ECMに格納された奇数鍵と偶数鍵とは同時に更新されずに、1つずつ順番に更新される。

【0040】秘匿化／非秘匿化情報、秘匿化に使用したスクランブル鍵の種別（奇数鍵／偶数鍵）情報は、可変長パケット単位に付加することが可能である。これら秘匿化に関する情報は、可変長パケットのヘッダに秘匿化情報203として格納される。

【0041】この発明の実施の形態1による限定受信方式では、多重化遅延に関する優先多重化を行なうために、パケットが生成されてから多重化されるまでの遅延時間（多重化遅延）がコンテンツ毎に異なる。それゆえ、受信側では古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが混在するのを防止する必要があるが、式1を満足するように秘匿化・優先多重化制御部4においてスクランブル鍵の更新周期やECMの更新タイミングを制御するのみではデスクランブルエラーが生じ得る。そこで、多重化されるビット列の最大多重化遅延 T_{dmx} を考慮して、

（式2）

【0044】以上のように、この発明の実施の形態1によれば、各コンテンツ毎の情報源符号化ビット列102を可変長パケット化した後に多重化して多重化ビット列104を生成するようにしたので、パケットを可変長に形成することができて固定長パケットのようにダミーバイトを挿入する必要がないから、多重化の効率を向上することができるという効果を奏する。

【0045】また、多重化されるビット列の最大多重化遅延時間よりもスクランブル鍵の更新周期を大きくとることで、受信側において古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが混在するのが防止されるから、符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。

【0046】また、秘匿化・優先多重化制御部4により、コンテンツに応じて、あるいはコンテンツ毎の情報源符号化モードに応じて秘匿化の優先度を設定する構成

とすることで、コンテンツあるいはコンテンツ毎の情報源符号化モードに応じた柔軟な秘匿特性を設定できるから、伝送するコンテンツの内容や用途に応じた柔軟な秘匿機能を実現できるという効果を奏する。

【0047】また、秘匿化・優先多重化制御部4が秘匿化についての優先度に基づき、暗号の種類および暗号の利用モードを変えて暗号化するように構成したので、コンテンツの内容または情報源符号化モード等に応じて秘匿の強度を適応的に制御することができるという効果を奏する。

【0048】さらに、秘匿化・優先多重化制御部4が秘匿化についての優先度に基づき、秘匿化期間を制御するように構成したので、コンテンツの内容または情報源符号化モード等に応じて、一定の期間中、契約者のみ復号可能にすること、あるいは受信者すべてに復号可能にすること等を選別して実施することができるから、受信形態を柔軟に設定することができるという効果を奏する。

【0049】実施の形態2、この発明の実施の形態2による限定受信方式の送信装置および受信装置は、実施の形態1による限定受信方式の送信装置および受信装置と基本的には同じ構造を有しており、その送信装置の構成は同様に図1により示され、また受信装置の構成は同様に図2により示される。実施の形態2は、実施の形態1と比較すると、可変長パケットの構成が異なる点でのみ相違する。

【0050】図5は、この発明の実施の形態2により使用される可変長パケットの構成を示す図である。図3に示される実施の形態1により使用される可変長パケットと比較すると、ECMバージョン番号208を有する点で相違している。ECMバージョン番号(ECM特定番号)208は、ECM識別番号(ECM特定番号)204で識別されるそれぞれの種別のECMについて、所定の秘匿化特性を付与されて個別化された個々のECMを特定するためのバージョン番号として与えられるものであり、それぞれの種別のECMにおいて内容の更新が生じた場合には、ECMバージョン番号が1ずつ増分される。

【0051】次に、動作について説明する。基本的な動作については実施の形態1と同様であるので、ここでは実施の形態1と相違する点について説明する。第1に、秘匿化の際には、秘匿化・優先多重化制御部4から出力される制御信号105により、実施の形態1と同様に適用されたスクランブル処理に係るECMの種別を識別するための番号がECM識別番号204のフィールドに書き込まれ、さらにこの実施の形態2ではスクランブル処理に使用されたスクランブル鍵が格納された個別のECMを特定するためのバージョン番号がECMバージョン番号208のフィールドに書き込まれる。

【0052】第2に、秘匿化解除の際には、可変長パケット分解・デスクランブル部6は、ECM識別番号20

4およびECMバージョン番号208により特定されるECMと、秘匿化情報203とを参照して、当該可変長パケットのスクランブル処理に使用されたスクランブル鍵を特定することにより、可変長パケットのペイロードの秘匿を解除する。

【0053】以上のように、この発明の実施の形態2によれば、実施の形態1と同様に多重化の効率の向上、柔軟な秘匿機能の実現という効果を奏するとともに、各可変長パケットがECMバージョン番号を格納するフィールドをヘッダに備えることで、当該可変長パケットのスクランブル処理に使用されたスクランブル鍵を特定することができるので、古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが受信側で混在しても符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。

【0054】実施の形態3

図6は、この発明の実施の形態3による限定受信方式の送信装置の構成を示すブロック図である。また、図7は、この発明の実施の形態3による限定受信方式の受信装置の構成を示すブロック図である。図6において、図1と同一符号は同一または相当部分を示すのでその説明を省略する。また、図7において、図2と同一符号は同一または相当部分を示すのでその説明を省略する。実施の形態3は、実施の形態1と比較すると、符号化ユニットを固定長パケットに格納して多重化する点で相違する。

【0055】図6において、10は固定長パケット化および秘匿化を実施する固定長パケット化・スクランブル部(パケット化・スクランブル手段)、106は固定長パケット列(パケット列)である。また、図7において、11は秘匿を解除するとともに固定長パケットを分解して情報源符号化ビット列102を生成する固定長パケット分解・デスクランブル部(パケット分解・デスクランブル手段)である。

【0056】次に動作について説明する。第1に、この発明の実施の形態3による限定受信方式の送信装置における処理について説明する。なお、情報源符号化部1、優先多重化部3、および秘匿化・優先多重化制御部4の動作は実施の形態1におけるのと同様であるので、その説明を省略する。

【0057】固定長パケット化・スクランブル部10は、それぞれの情報源符号化ビット列102を符号化ユニット毎に分割して固定長パケットのペイロードに格納し固定長パケットを生成するとともに、固定長パケットのペイロードをスクランブル処理して秘匿化し固定長パケット列106を生成する。情報源符号化ビット列102を固定長パケットのペイロードに格納する際には、図12に示すように情報源符号化ユニットの先頭部が常に固定長パケットのペイロードの先頭部に一致するように

処理がなされる。このために、固定長パケットのペイロードにはダミーバイトが挿入される。

【0058】図8は、この発明の実施の形態3により使用される固定長パケットの構成を示す図である。301は固定長パケットの先頭を示すパケットスタートコード、302はパケットに格納されるコンテンツ毎に異なる番号が付与されるパケット識別子、303は秘匿化／非秘匿化情報、秘匿化に使用する奇数鍵／偶数鍵の区別情報、C B CやO F B等の暗号の利用モード等を通知する秘匿化情報、304は当該固定長パケットの秘匿化に係るECMを格納する固定長パケットのパケット識別子の値を通知するECM識別番号、305は固定長パケットのペイロードに格納されたコンテンツとダミーバイトとを区別するための有効バイト長、307は符号化されたコンテンツを格納する固定長パケットペイロードである。

【0059】なお、秘匿化に関して個々の固定長パケットの秘匿化情報303のフィールドに収容されないスクランブル鍵等の秘匿化関連情報は、ECMとして固定長パケットのペイロードに格納して送られる。

【0060】第2に、この発明の実施の形態3による限定受信方式の受信装置における処理について図7を参照して説明する。図7に示されるように、優先多重分離部5は、パケットスタートコード301、パケット識別子302、および有効バイト長305を参照して、多重化ビット列104をコンテンツ毎に分離して固定長パケット列106を生成する。

【0061】次に、固定長パケット分解・デスクランブル部11は、秘匿化情報303とECM識別情報304により同定されたECMとを参照して固定長パケットのペイロードの秘匿を解除するとともに、固定長パケットを分解してコンテンツ毎の情報源符号化ビット列102を生成する。そして、情報源復号部7は情報源符号化ビット列102を復号して映像信号、音声信号、種々のデータ等のコンテンツ101を再生する。

【0062】なお、この発明の実施の形態3による限定受信方式における伝送信号の多重方式、及び秘匿化・優先多重化制御部4の動作については、実施の形態1と同様であるのでその説明を省略する。

【0063】以上のように、この発明の実施の形態3によれば、多重化されるビット列の最大多重化遅延時間よりもスクランブル鍵の更新周期を大きくとることで、受信側において古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが混在するのが防止されるので、符号化ビット列の復号を確実に実施でき、限定受信方式における信頼性を高めることができるという効果を奏する。

【0064】さらに、秘匿化・優先多重化制御部4により、コンテンツに応じて、あるいはコンテンツ毎の情報源符号化モードに応じて秘匿化の優先度を設定する構成

とすることで、コンテンツあるいはコンテンツ毎の情報源符号化モードに応じた柔軟な秘匿特性を設定できるから、伝送するコンテンツの内容や用途に応じた柔軟な秘匿機能を実現できるという効果を奏する。

【0065】実施の形態4、この発明の実施の形態4による限定受信方式の送信装置および受信装置は、実施の形態3による限定受信方式の送信装置および受信装置と基本的には同じ構造を有しており、その送信装置の構成は同様に図6により示され、また受信装置の構成は同様に図7により示される。実施の形態4は、実施の形態3と比較すると、固定長パケットの構成が異なる点でのみ相違する。

【0066】図9は、この発明の実施の形態4により使用される固定長パケットの構成を示す図である。図8に示される実施の形態3により使用される固定長パケットと比較すると、ECMバージョン番号308を有する点で相違している。ECMバージョン番号308は、ECM識別番号304で識別されるそれぞれの種別のECMについて、所定の秘匿化特性を付与されて個別化された個々のECMを特定するためのバージョン番号として与えられるものであり、それぞれの種別のECMにおいて内容の更新が生じた場合には、ECMバージョン番号が1ずつ増分される。

【0067】次に、動作について説明する。基本的な動作については実施の形態3と同様であるので、ここでは実施の形態3と相違する点について説明する。第1に、秘匿化の際には、秘匿化・優先多重化制御部4から出力される制御信号105により、実施の形態3と同様に、適用されたスクランブル処理に係るECMの種別を識別するための番号がECM識別番号304のフィールドに書き込まれ、さらにこの実施の形態4ではスクランブル処理に使用されたスクランブル鍵が格納された個別のECMを特定するためのバージョン番号がECMバージョン番号308のフィールドに書き込まれる。

【0068】第2に、秘匿化解除の際には、固定長パケット分解・デスクランブル部11は、ECM識別番号304およびECMバージョン番号308により特定されるECMと、秘匿化情報303とを参照して、当該固定長パケットのスクランブル処理に使用されたスクランブル鍵を特定することにより、固定長パケットのペイロードの秘匿を解除する。

【0069】以上のように、この発明の実施の形態4によれば、実施の形態3と同様に多重化の効率の向上、柔軟な秘匿機能の実現という効果を奏するとともに、各固定長パケットがECMバージョン番号を格納するフィールドをヘッダに備えることで、当該固定長パケットのスクランブル処理に使用されたスクランブル鍵を特定することができるので、古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが受信側で混在しても符号化ビット列の復号を確実に実施でき

て、限定受信方式における信頼性を高めることができるという効果を奏する。

【0070】

【発明の効果】以上のように、この発明によれば、秘匿化・優先多重化制御手段が多重化ビット列において最大多重化遅延時間よりも大きな時間間隔でスクランブル鍵を更新するように制御する構成としたので、受信側において古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが混在するのが防止されるから、符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。

【0071】この発明によれば、パケット化・スクランブル手段が情報源符号化ビット列を可変長パケットのペイロードに格納して可変長パケットを生成するように構成したので、固定長パケットのようにダミーバイトを挿入する必要がなく多重化の効率を向上することができるという効果を奏する。

【0072】この発明によれば、パケット化・スクランブル手段がパケットの一部分を秘匿化するために使用したスクランブル鍵を格納するECMを特定するためのECM特定番号をパケットのヘッダに登録するように構成したので、当該パケットのスクランブル処理に使用されたスクランブル鍵を特定することができるから、古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが受信側で混在しても符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。

【0073】この発明によれば、パケット分解・デスクランブル手段が、ECM特定番号を参照して、パケットの一部分を秘匿化するために使用したスクランブル鍵を特定し、パケットの秘匿化部分の秘匿を解除するように構成したので、古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが受信側で混在しても符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。

【0074】この発明によれば、秘匿化・優先多重化制御手段が秘匿化についての優先度に基づいてパケットの秘匿特性を制御するように構成したので、各種コンテンツに応じて、あるいはコンテンツ毎の情報源符号化モードに応じて柔軟な秘匿特性を設定できるから、伝送するコンテンツの内容あるいは情報源符号化モードに応じた柔軟な秘匿機能を実現できるという効果を奏する。

【0075】この発明によれば、秘匿化・優先多重化制御手段が秘匿化についての優先度に基づき、暗号の種類、およびCBCモードやOFBモード等の暗号の利用モードを変えて暗号化するように構成したので、コンテンツの内容または情報源符号化モード等に応じて秘匿の強度を適応的に制御することができるという効果を奏す

る。

【0076】この発明によれば、秘匿化・優先多重化制御手段が秘匿化についての優先度に基づき、秘匿化期間を制御するように構成したので、コンテンツの内容または情報源符号化モード等に応じて、一定の期間中、契約者のみ復号可能にすること、あるいは受信者すべてに復号可能にすること等を選別して実施することができるから、受信形態を柔軟に設定することができるという効果を奏する。

10 【図面の簡単な説明】

【図1】この発明の実施の形態1による限定受信方式の送信装置の構成を示すブロック図である。

【図2】この発明の実施の形態1による限定受信方式の受信装置の構成を示すブロック図である。

【図3】この発明の実施の形態1による限定受信方式で使用される可変長パケットの構成を示す図である。

【図4】この発明の実施の形態1による限定受信方式における伝送信号の多重方式を説明する図である。

20 【図5】この発明の実施の形態2による限定受信方式で使用される可変長パケットの構成を示す図である。

【図6】この発明の実施の形態3による限定受信方式の送信装置の構成を示すブロック図である。

【図7】この発明の実施の形態3による限定受信方式の受信装置の構成を示すブロック図である。

20 【図8】この発明の実施の形態3による限定受信方式で使用される固定長パケットの構成を示す図である。

【図9】この発明の実施の形態4による限定受信方式で使用される固定長パケットの構成を示す図である。

30 【図10】従来の限定受信方式の送信装置の構成を示すブロック図である。

【図11】従来の限定受信方式の受信装置の構成を示すブロック図である。

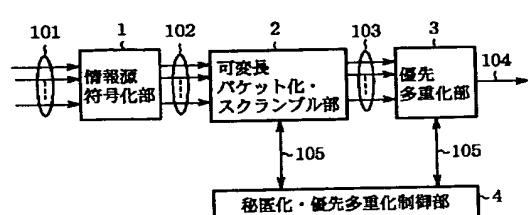
【図12】従来の限定受信方式における伝送信号の多重方式を説明する図である。

【符号の説明】

- 1 情報源符号化部（情報源符号化手段）、2 可変長パケット化・スクランブル部（パケット化・スクランブル手段）、3 優先多重化部（優先多重化手段）、4 秘匿化・優先多重化制御部（秘匿化・優先多重化制御手段）、5 優先多重分離部（優先多重分離手段）、6 可変長パケット分解・デスクランブル部（パケット分解・デスクランブル手段）、7 情報源復号部（情報源復号手段）、10 固定長パケット化・スクランブル部（パケット化・スクランブル手段）、11 固定長パケット分解・デスクランブル部（パケット分解・デスクランブル手段）、101 コンテンツ、102 情報源符号化ビット列、103 可変長パケット列（パケット列）、104 多重化ビット列、106 固定長パケット列（パケット列）、204 ECM識別番号（ECM特定番号）、208 ECMバージョン番号（ECM特

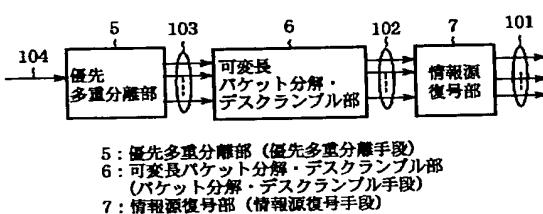
定番号)。

【図1】

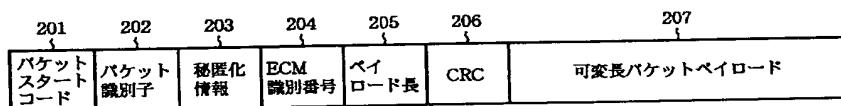


1: 情報源符号化部 (情報源符号化手段)
 2: 可変長パケット化・スクランブル部
 (パケット化・スクランブル手段)
 3: 優先多重化部 (優先多重化手段)
 4: 秘匿化・優先多重化制御部 (秘匿化・優先多重化制御手段)
 101: コンテンツ
 102: 情報源符号化ビット列
 103: 可変長パケット列 (パケット列)
 104: 多重化ビット列

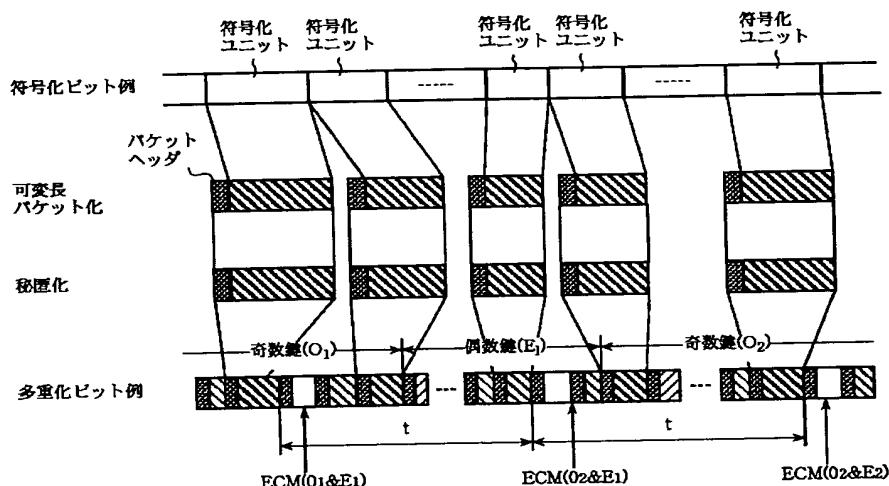
【図2】



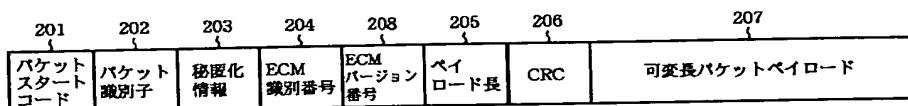
【図3】



【図4】



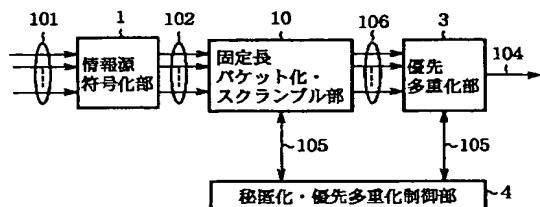
【図5】



204: ECM識別番号 (ECM特定番号)
 208: ECMバージョン番号 (ECM特定番号)

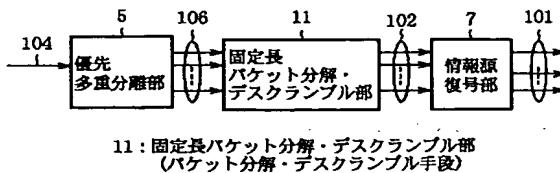
BEST AVAILABLE COPY

【図6】



10: 固定長パケット化・スクランブル部
(パケット化・スクランブル手段)
106: 固定長パケット列(パケット列)

【図7】

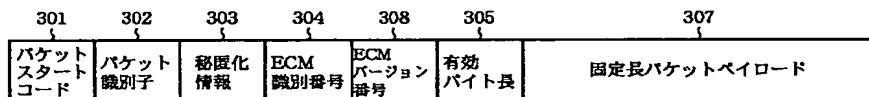


11: 固定長パケット分解・デスクランブル部
(パケット分解・デスクランブル手段)

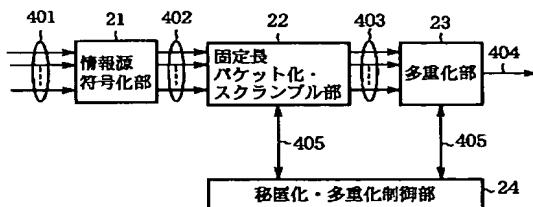
【図8】



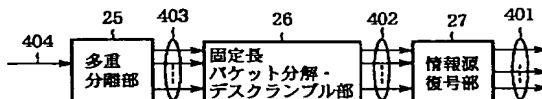
【図9】



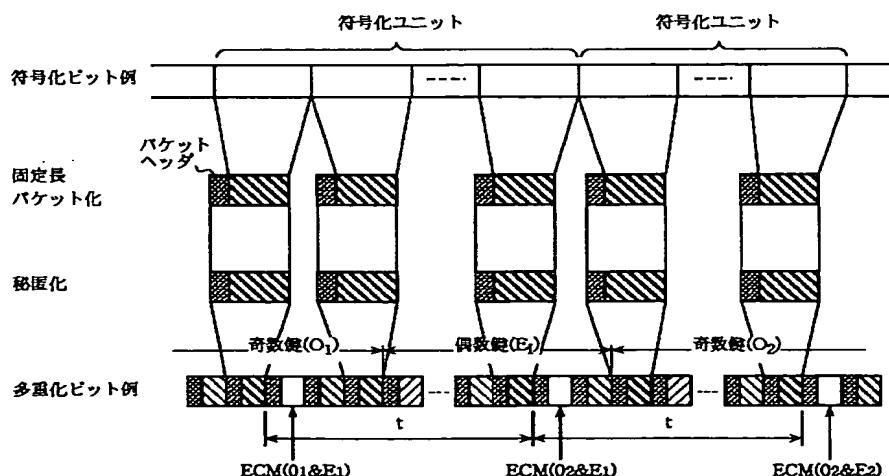
【図10】



【図11】



【図12】



フロントページの続き

(51)Int.Cl.⁷
H 04 N 7/167

識別記号

F I
H 04 N 7/167テーマコード(参考)
Z

F ターム(参考) 5C064 CA14 CC04
5J104 AA01 AA34 BA03 BA04 NA02
NA37 PA05
5K028 AA14 CC02 EE03 KK32 SS07
SS17 TT01
5K030 GA03 GA11 HA02 HC01 JA05
JT04 LD19

【公報種別】特許法第17条の2の規定による補正の掲載

【部門区分】第7部門第3区分

【発行日】平成17年7月21日(2005.7.21)

【公開番号】特開2000-332745(P2000-332745A)

【公開日】平成12年11月30日(2000.11.30)

【出願番号】特願平11-140340

【国際特許分類第7版】

H 04 L 9/14

H 04 H 1/00

H 04 J 3/00

H 04 L 12/56

H 04 N 7/167

【F I】

H 04 L 9/00 6 4 1

H 04 H 1/00 F

H 04 J 3/00 M

H 04 J 3/00 B

H 04 L 11/20 1 0 2 Z

H 04 N 7/167 Z

【手続補正書】

【提出日】平成16年12月1日(2004.12.1)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】特許請求の範囲

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項1】

各種のコンテンツを符号化する情報源符号化手段と、

該情報源符号化手段から出力される情報源符号化ビット列をパケットに格納するとともに該パケットの一部分を秘匿化してパケット列を生成するパケット化・スクランブル手段と、

複数の情報源符号化ビット列をパケット単位に多重化して多重化ビット列を生成する多重化手段と、

前記パケット化・スクランブル手段および前記多重化手段を制御する秘匿化・多重化制御手段とを有する限定受信方式の送信装置において、

前記秘匿化・多重化制御手段が、前記多重化ビット列において、最大多重化遅延時間よりも大きな時間間隔でスクランブル鍵を更新するように制御することを特徴とする限定受信方式の送信装置。

【請求項2】

パケット化・スクランブル手段が、情報源符号化ビット列を可変長パケットのペイロードに格納して可変長パケットを生成することを特徴とする請求項1記載の限定受信方式の送信装置。

【請求項3】

各種のコンテンツを符号化する情報源符号化手段と、

該情報源符号化手段から出力される情報源符号化ビット列をパケットに格納するとともに該パケットの一部分を秘匿化してパケット列を生成するパケット化・スクランブル手段と、

複数の情報源符号化ビット列をパケット単位に多重化して多重化ビット列を生成する多重化手段と、

前記パケット化・スクランブル手段および前記多重化手段を制御する秘匿化・多重化制御手段とを有する限定受信方式の送信装置において、

前記パケット化・スクランブル手段が、パケットの一部分を秘匿化するために使用したスクランブル鍵を格納するECMを特定するためのECM特定番号をパケットのヘッダで通知することを特徴とする限定受信方式の送信装置。

【請求項4】

パケット化・スクランブル手段が、情報源符号化ビット列を可変長パケットのペイロードに格納して可変長パケットを生成することを特徴とする請求項3記載の限定受信方式の送信装置。

【請求項5】

パケット単位に多重化された多重化ビット列をコンテンツ毎のパケット列に分離する多重分離手段と、

パケット列において秘匿化された部分の秘匿を解除するとともに、パケットを分解して情報源符号化ビット列を生成するパケット分解・デスクランブル手段と、

情報源符号化ビット列を復号してコンテンツを再生する情報源復号手段とを有する限定受信方式の受信装置において、

前記パケット分解・デスクランブル手段が、ECM特定番号を参照して、パケットの一部分を秘匿化するために使用したスクランブル鍵を特定し、パケットの秘匿化部分の秘匿を解除することを特徴とする限定受信方式の受信装置。

【請求項6】

各種のコンテンツを符号化する情報源符号化手段と、

該情報源符号化手段から出力される情報源符号化ビット列をパケットに格納して該パケットの一部分を秘匿化するパケット化・スクランブル手段と、

複数の情報源符号化ビット列をパケット単位に多重化して多重化ビット列を生成する多重化手段と、

前記パケット化・スクランブル手段および前記多重化手段を制御する秘匿化・多重化制御手段とを有する限定受信方式の送信装置において、

前記秘匿化・多重化制御手段が、秘匿化についての優先度に基づいてパケットの秘匿特性を制御することを特徴とする限定受信方式の送信装置。

【請求項7】

秘匿化・多重化制御手段は、コンテンツ毎の情報源符号化モード単位に設定された秘匿化についての優先度に基づいてパケットの秘匿特性を制御することを特徴とする請求項6記載の限定受信方式の送信装置。

【請求項8】

秘匿化・多重化制御手段は、秘匿化についての優先度に基づき、暗号の種類、およびCBCモードやOFBモード等の暗号の利用モードを変えて暗号化することを特徴とする請求項6または請求項7に記載の限定受信方式の送信装置。

【請求項9】

秘匿化・多重化制御手段は、秘匿化についての優先度に基づき、秘匿化期間を制御することを特徴とする請求項6または請求項7に記載の限定受信方式の送信装置。

【請求項10】

パケット化・スクランブル手段が、情報源符号化ビット列を可変長パケットのペイロードに格納して可変長パケットを生成することを特徴とする請求項6から請求項9のいずれか1項に記載の限定受信方式の送信装置。

【請求項11】

多重化手段は、複数の情報源符号化ビット列を該情報源符号化ビット列毎に与えられた多重化手段に基づく優先度に基づいてパケット単位に多重化して多重化ビット列を生成することを特徴とする請求項1または請求項3または請求項6に記載の限定受信方式の送信

装置。

【手続補正 2】

【補正対象書類名】明細書

【補正対象項目名】0016

【補正方法】変更

【補正の内容】

【0016】

【課題を解決するための手段】

この発明に係る限定受信方式の送信装置は、秘匿化・多重化制御手段が多重化ビット列において、最大多重化遅延時間よりも大きな時間間隔でスクランブル鍵を更新するように制御するものである。

【手続補正 3】

【補正対象書類名】明細書

【補正対象項目名】0018

【補正方法】変更

【補正の内容】

【0018】

この発明に係る限定受信方式の送信装置は、パケット化・スクランブル手段がパケットの一部分を秘匿化するために使用したスクランブル鍵を格納するECMを特定するためのECM特定番号をパケットのヘッダで通知するようにしたものである。

【手続補正 4】

【補正対象書類名】明細書

【補正対象項目名】0020

【補正方法】変更

【補正の内容】

【0020】

この発明に係る限定受信方式の送信装置は、秘匿化・多重化制御手段が秘匿化についての優先度に基づいてパケットの秘匿特性を制御するようにしたものである。

【手続補正 5】

【補正対象書類名】明細書

【補正対象項目名】0021

【補正方法】変更

【補正の内容】

【0021】

この発明に係る限定受信方式の送信装置は、秘匿化・多重化制御手段がコンテンツ毎の情報源符号化モード単位に設定された秘匿化についての優先度に基づいてパケットの秘匿特性を制御するようにしたものである。

【手続補正 6】

【補正対象書類名】明細書

【補正対象項目名】0022

【補正方法】変更

【補正の内容】

【0022】

この発明に係る限定受信方式の送信装置は、秘匿化・多重化制御手段が秘匿化についての優先度に基づき、暗号の種類、およびCBCモードやOFBモード等の暗号の利用モードを変えて暗号化するようにしたものである。

【手続補正 7】

【補正対象書類名】明細書

【補正対象項目名】0023

【補正方法】変更

【補正の内容】**【0023】**

この発明に係る限定受信方式の送信装置は、秘匿化・多重化制御手段が秘匿化についての優先度に基づき秘匿化期間を制御するようにしたものである。

この発明に係る限定受信方式の送信装置は、多重化手段が、複数の情報源符号化ビット列を該情報源符号化ビット列毎に与えられた多重化遅延に基づく優先度に基づいてパケット単位に多重化して多重化ビット列を生成するようにしたものである。

【手続補正8】

【補正対象書類名】明細書

【補正対象項目名】0070

【補正方法】変更

【補正の内容】**【0070】****【発明の効果】**

以上のように、この発明によれば、秘匿化・多重化制御手段が多重化ビット列において最大多重化遅延時間よりも大きな時間間隔でスクランブル鍵を更新するように制御する構成としたので、受信側において古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが混在するのが防止されるから、符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。

【手続補正9】

【補正対象書類名】明細書

【補正対象項目名】0072

【補正方法】変更

【補正の内容】**【0072】**

この発明によれば、パケット化・スクランブル手段がパケットの一部分を秘匿化するためには、ECMを特定するためのECM特定番号をパケットのヘッダで通知するように構成したので、当該パケットのスクランブル処理に使用されたスクランブル鍵を特定することができるから、古い鍵でスクランブルされたパケットと新しい鍵でスクランブルされたパケットとが受信側で混在しても符号化ビット列の復号を確実に実施できて、限定受信方式における信頼性を高めることができるという効果を奏する。

【手続補正10】

【補正対象書類名】明細書

【補正対象項目名】0074

【補正方法】変更

【補正の内容】**【0074】**

この発明によれば、秘匿化・多重化制御手段が秘匿化についての優先度に基づいてパケットの秘匿特性を制御するように構成したので、各種コンテンツに応じて、あるいはコンテンツ毎の情報源符号化モードに応じて柔軟な秘匿特性を設定できるから、伝送するコンテンツの内容あるいは情報源符号化モードに応じた柔軟な秘匿機能を実現できるという効果を奏する。

【手続補正11】

【補正対象書類名】明細書

【補正対象項目名】0075

【補正方法】変更

【補正の内容】**【0075】**

この発明によれば、秘匿化・多重化制御手段が秘匿化についての優先度に基づき、暗号

の種類、およびCBCモードやOFBモード等の暗号の利用モードを変えて暗号化するように構成したので、コンテンツの内容または情報源符号化モード等に応じて秘匿の強度を適応的に制御することができるという効果を奏する。

【手続補正12】

【補正対象書類名】明細書

【補正対象項目名】0076

【補正方法】変更

【補正の内容】

【0076】

この発明によれば、秘匿化・多重化制御手段が秘匿化についての優先度に基づき、秘匿化期間を制御するように構成したので、コンテンツの内容または情報源符号化モード等に応じて、一定の期間中、契約者のみ復号可能にすること、あるいは受信者すべてに復号可能にすること等を選別して実施することができるから、受信形態を柔軟に設定することができるという効果を奏する。

THIS PAGE BLANK (USPTO)